Clean Copy of the Currently Pending Claims

1. A method for automatically disbursing a first party's personal information to a receiving party authorized by the first party by transmitting said first party's personal information from a server computer operated by a service provider, said server computer coupled to a database, the method comprising the steps of:

establishing an account for the first party with the server computer;

assigning an identifier to the first party;

entering the first party's personal information, said first party's personal information comprising at least one of a plurality of information objects;

assigning at least one of a plurality of security levels to each information object at any granularity, thereby enabling access to individually selected portions of the first party's personal information by individual receiving parties;

storing in the database the first party identifier, the information object and the security level assigned to the information object;

receiving a request, said request comprising at least the first party identifier;

in response to the request, selecting a first portion of the first party's personal information objects that could be transmitted to a second party;

retrieving from the database the selected first portion of personal information objects; and

securely transmitting the retrieved first portion of personal information objects to the second party.

2. The method of claim 1, further comprising the steps of:

presenting an authorization by the second party; and

verifying the second party's authorization.

3. The method of claim 2, further comprising the steps of:

obtaining a second party identifier;

if the second party is not authorized to receive the information, recording the second party identifier; and

rejecting the second party's request for information.

4. The method of claim 3, further comprising the steps of:

designating the second party as a junk requester if the second party presents a predetermined number of requests that are not authorized; and

generating an alarm indication.

g1 cont

5. The method of claim 1, further comprising the step of recording every access of the first party's personal information to create an audit trail.

7. The method of claim 1, further comprising the steps of:

generating an authorization key; and

providing the authorization key to the second party.

8. The method of claim 7, wherein the step of generating an authorization key comprises the steps of:

selecting at least one set of information objects, the set of selected information objects comprising at least one piece of the first party's personal information; and

creating a key to authorize access of the selected set of information objects.

9. The method of claim 7, wherein the step of generating an authorization key comprises the step of:

selecting the characteristics of second party that can present the authoization key for information.

10. The method of claim 7, further comprising the step of:

encoding the authorization key with at least one of a plurality of attributes.

11. The method of claim 10, wherein the at least one of a plurality of attributes includes an attribute of a the second party who may present the authorization key to access the first party's information.

14. The method of claim 1, further comprising the steps of:

altering the first party's personal information; and

storing said altered personal information in the database.

15. The method of claim 14, wherein the step of transmitting further comprises the step of:

designating an entity to receive said altered personal information;

optionally designating an effective date for said alteration; and

transmitting the altered personal information to the designated entity.

16. The method of claim 1, wherein the step of securely transmitting the information object comprises the step of:

transmitting the information object via a communication network to a device coupled to the communication network.

17. The method of claim 16, wherein the device is a printer coupled to the communication network directly via the Internet Printing Protocol.

18. The method of claim 1, wherein the step of securely transmitting the information object further comprises the step of:

transmitting the information object via secure E-mail or public key encryption.

19. The method of claim 1, wherein the first party's personal information includes the first party's contact information; health-related information; medical, dental, information; credit/employment information; insurance information; property-related information; personal demographic information; family medical history; biometric/genetic information; travel/hotel preferencfes; internet preferences; sartorial, fashion preferences; magazine, movies, book preferences; leisure preferences; preferences for billing or payment methods, or pleasure-related preferences.

21 cont

20. The method of claim 1, further comprising the step of:

receiving an authorization key from the second party.

21. The method of claim 1, further comprising the step of:

authenticating the second party.

22. The method of claim 1, wherein the step of receiving a request message from the second party comprises the step of:

receiving a query for the first party's personal information in a readily executable form.

23. The method of claim 1, wherein the step of receiving a request message from the second party comprises the step of:

receiving a query for the first party's personal information in a readily executable form.

24. The method of claim 1, further comprising the step of:

periodically generating a report on the transmittal of the information.

26. A program storage device readable by a processor, said storage device tangibly embodying a program of instructions executable by the processor to perform the method steps for secure delivery of a first party's personal information via a communication network, said method steps comprising:

storing the first party's personal information, said first party's personal information comprising at least one of a plurality of information objects;

associating each information object with at least one of a plurality of security clearance levels at any granularity;

E1 cont

receiving a request message to access the first party's personal information, said request message comprising an authorization key to access a first portion of the first party's personal information, said authorization key indicative of a second security clearance level;

comparing the first security clearance level and the second security clearance level to determine an appropriate overall clearance level;

matching the request message and the overall clearance level with a second portion of the first party's personal information; and

securely transmitting the second portion of the first party's personal information.

27. The program storage device of claim 26, further comprising program of instructions executable by the processor to perform the method steps of:

authenticating the request message.

28. The program storage device of claim 26, further comprising program of instructions executable by the processor to perform the method step of:

establishing a secure audit trail of each access of the first party's personal information.

29. The program storage device of claim 28, wherein the program of

instructions executable by the processor to perform the method step of establishing a secure audit trail include program of instructions executable by the processor to perform the method step of recording an identifier to identify a party that receives the first party's personal information.

30. The program storage device of claim 28, wherein the program of instructions executable by the processor to perform the method step of establishing the secure audit trail include program of instructions executable by the processor to perform the method step of recording an identifier to identify a second party.

Cont

44. The method of claim 1, further comprising the step of:
generating an authorization key;
providing the authorization key to the second party; and
encoding the authorization key with at least one of a plurality of criteria.

45. The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion to indicate the information that can be accessed by the second party with the authorization key.

46. The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion to indicate the number of times the authorization key can be used by the second party to obtain access.

47. The method of claim 44, wherein the at least one of a plurality of criteria includes a criterion designating the category of the first party's personal information that can be accessed by the second party using the authorization key.